# FortiAnalyzer

Version 5.4

QuickStart Guide

# REGISTER FOR SUPPORT

## REGISTER YOUR FORTINET PRODUCT TO RECEIVE:

- Technical Support
- New product features
- Protection from new threats

## LA REISTRAZIONE TI PERMETTE DI USUFRUIRE DI:

- Supporto Tecnico
- Nuove funzionalita
- Proteezione dalle ultime minaccce

## VOUS DEVEZ ENREGISTRER LE PRODUIT POUR RECEVOIR:

- Support technique
- Nouvelles fonctionnalitées du produit
- Protection contre de nouvelles menaces

## DEBE REGISTRAR EL PRODUCTO PARA RECIBIR:

- Apoyo técnico
- Nuevas funcionalidades del producto
- Protección contra ataques

## 登録のお願い

本日、フォーティネット製品の登録をしてください。
登録すると次のメリットがあります。
テクニカルサポート・新機能の追加・新しい脅威への防御

## 请马上注册

您的飞塔产品
您在注册以后才能得到技术支持、新产品特点信息、最新威胁防护

## SUPPORT

http://forti.net/support

Toll free: 1 866 648 4638

Phone: 1 408 486 7899

Fax: 1 408 235 7737

November 03, 2016

OS-541-370731-20160513



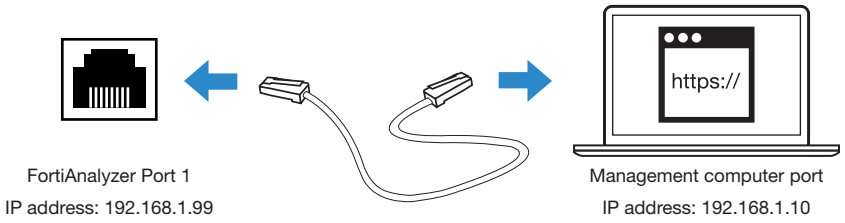
# DAY1: SETUP

- Configure network settings and admin account
- Set up FortiGate to send logs
- View logs from Log View

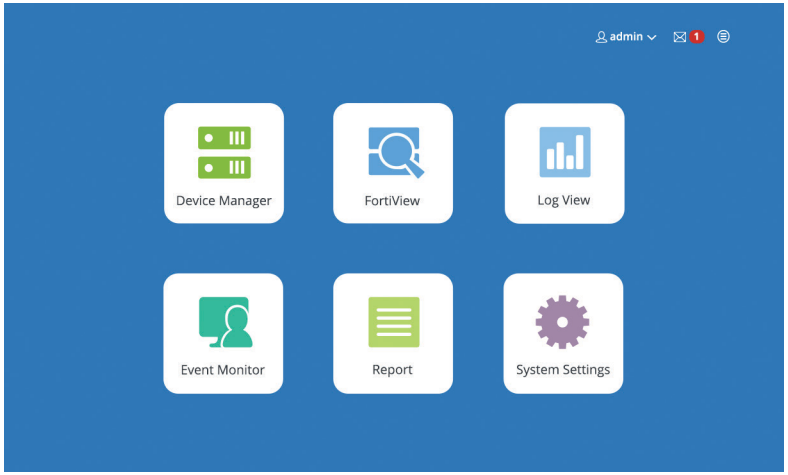
# 1 Set Up FortiAnalyzer

## Configure FortiAnalyzer Network Settings

1. Connect the FortiAnalyzer **Port 1** to the **Management computer port**.



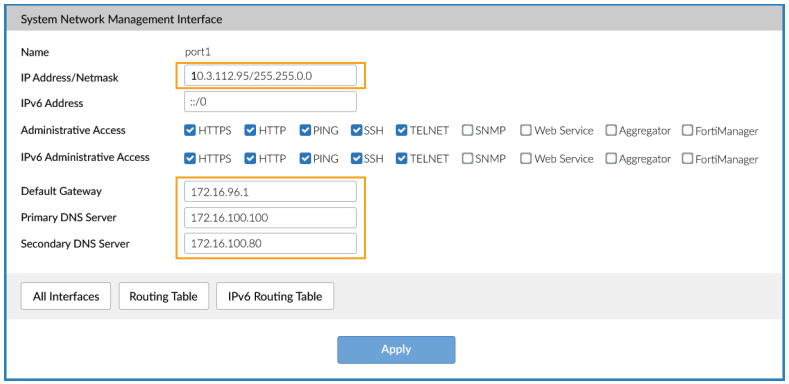

2. Set the management computer to be on the same subnet as FortiAnalyzer. (The default is 192.168.1.99.)
   For Example:
   IP Address: 192.168.1.10
   Netmask: 255.255.255.0
3. Visit https://192.168.1.99 in your web browser.
4. Log in with username **admin** and no password.





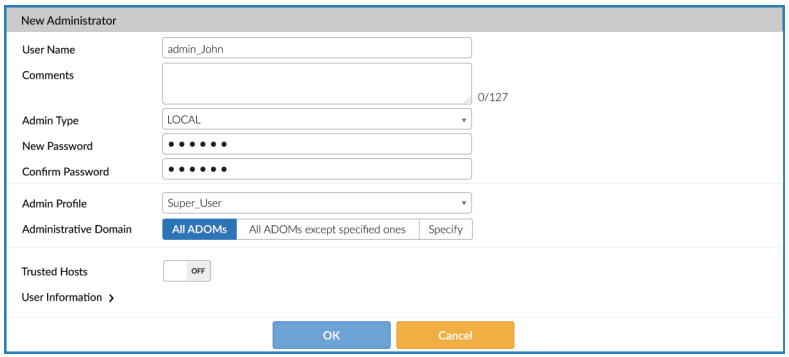

## Configure FortiAnalyzer Network Settings

1. Go to **System Settings > Network**.
2. Change the **IP address/Netmask** to your internal network.
3. Keep the default **Administrative Access** settings.
4. Specify a **Default Gateway**.
5. Change the IP address/Netmask of the management computer accordingly to reconnect it to FortiAnalyzer.



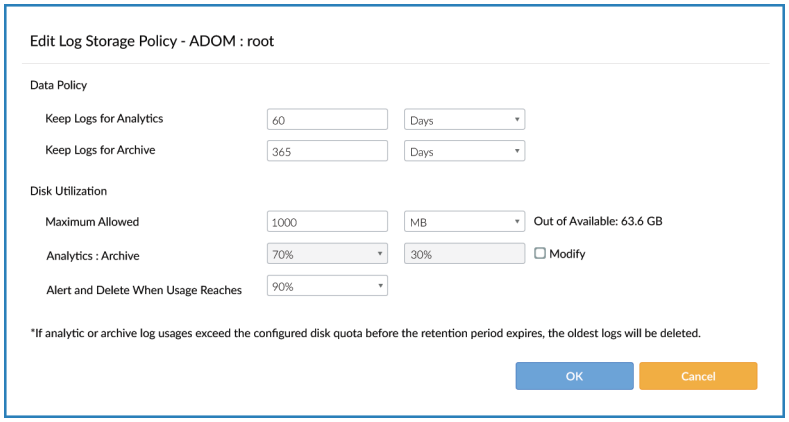

## Set Up Administrator Accounts

1. Go to **System Settings > Admin > Administrator**, and click **Create New** in the toolbar.
2. Enter user name and password.
3. Click **OK** to save the change.



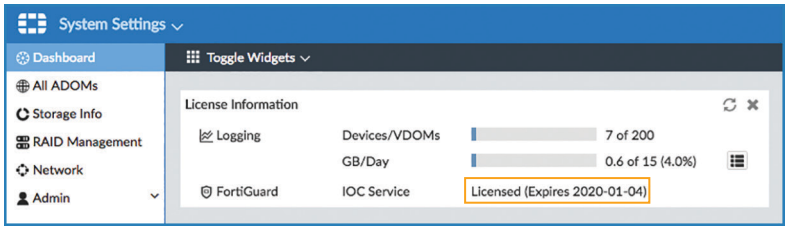
## Configure Log Storage Policy

1. Go to **System Settings > Dashboard**.
2. In the **System Information** widget, under **Log Storage Policy**, select **Edit Log Storage policy**.
   - Data Policy:
     - Set **Keep Logs for Analytics** to **90 days**.
     - Set **Keep Logs for Archive** to **180 days**.
   - Disk Utilization:
     - Keep the default values.




You can monitor the log storage settings and adjust as you go.

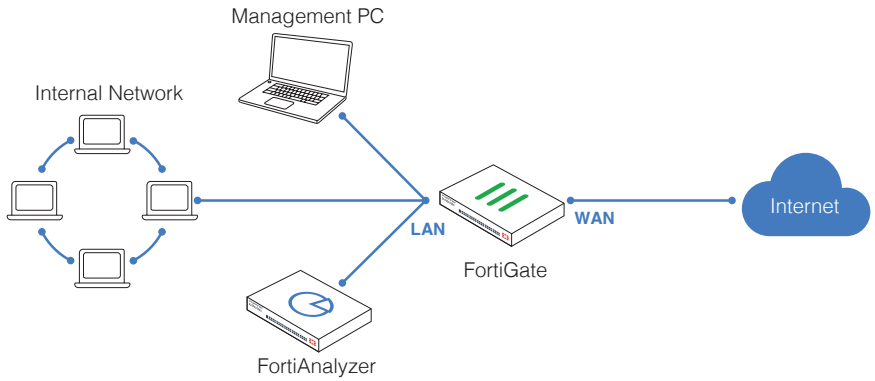
## Check License and Registration




Check that you have a valid license for the **IOC Service**, to enable the feature.

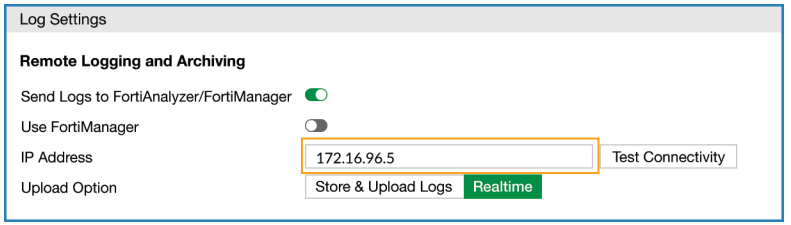


# 2 Connect FortiGate to FortiAnalyzer




## Configure FortiGate Log Settings

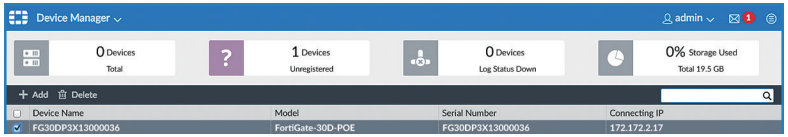
1. Log in to the FortiGate GUI from the management computer.
2. Go to **Log & Report > Log Settings**.
   - Turn on **Send Logs to FortiAnalyzer/FortiManager**.
   - Enter the IP address of the FortiAnalyzer and click **Apply**.



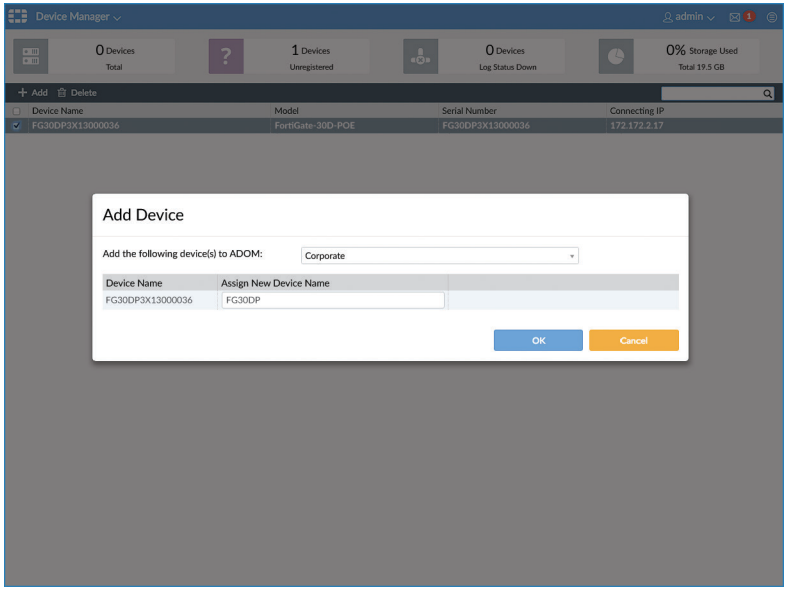

Don't click **Test Connectivity** yet. You need to register this FortiGate on the FortiAnalyzer first.

## Register FortiGate on FortiAnalyzer

1. Go to **Device Manager** of FortiAnalyzer. Click the **Unregistered Devices** tab in the quick status bar.

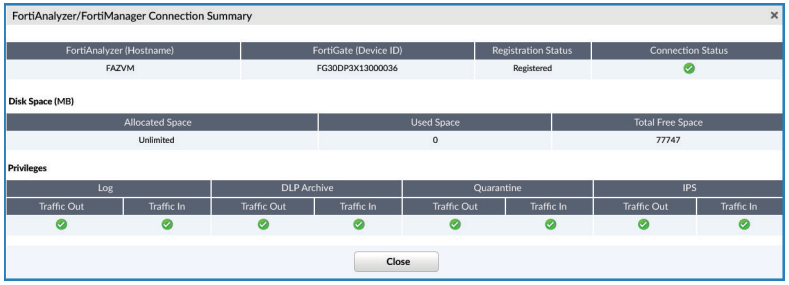



2. Select the FortiGate device, and click **Add**.
3. In the Add Device dialog box that opens, select the root ADOM, type a device name, and click **OK**.



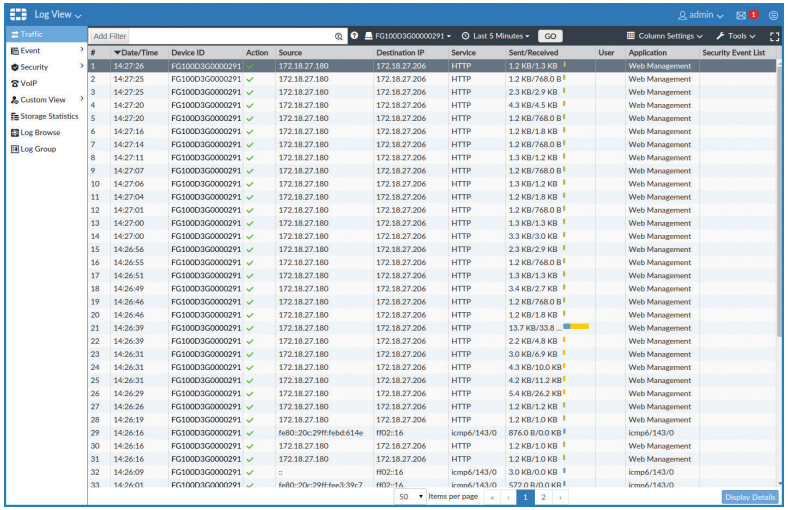

## Test Connectivity on FortiGate

1. Go back to the Log Settings pane of FortiGate, and click **Test Connectivity**. If the connection is successfully established, a connection summary is shown.




## Verify Logs Being Received

1. Go to **Log View** of the FortiAnalyzer. Select **Last 5 minutes** from the time period list and press **GO**. You should be able to see the FortiGate logs.



# DAY 2: NAVIGATE

- Interact with FortiView
- Generate reports
- Monitor events

## 1 Look into FortiView Summaries

In FortiView, the Summary view provides different Fortinet summaries as widgets. You can customize the widgets being displayed, and also drill down into each widget for further info.

### Fortiview Summary

Source IP 172.16.100.80 used the most bandwidth.

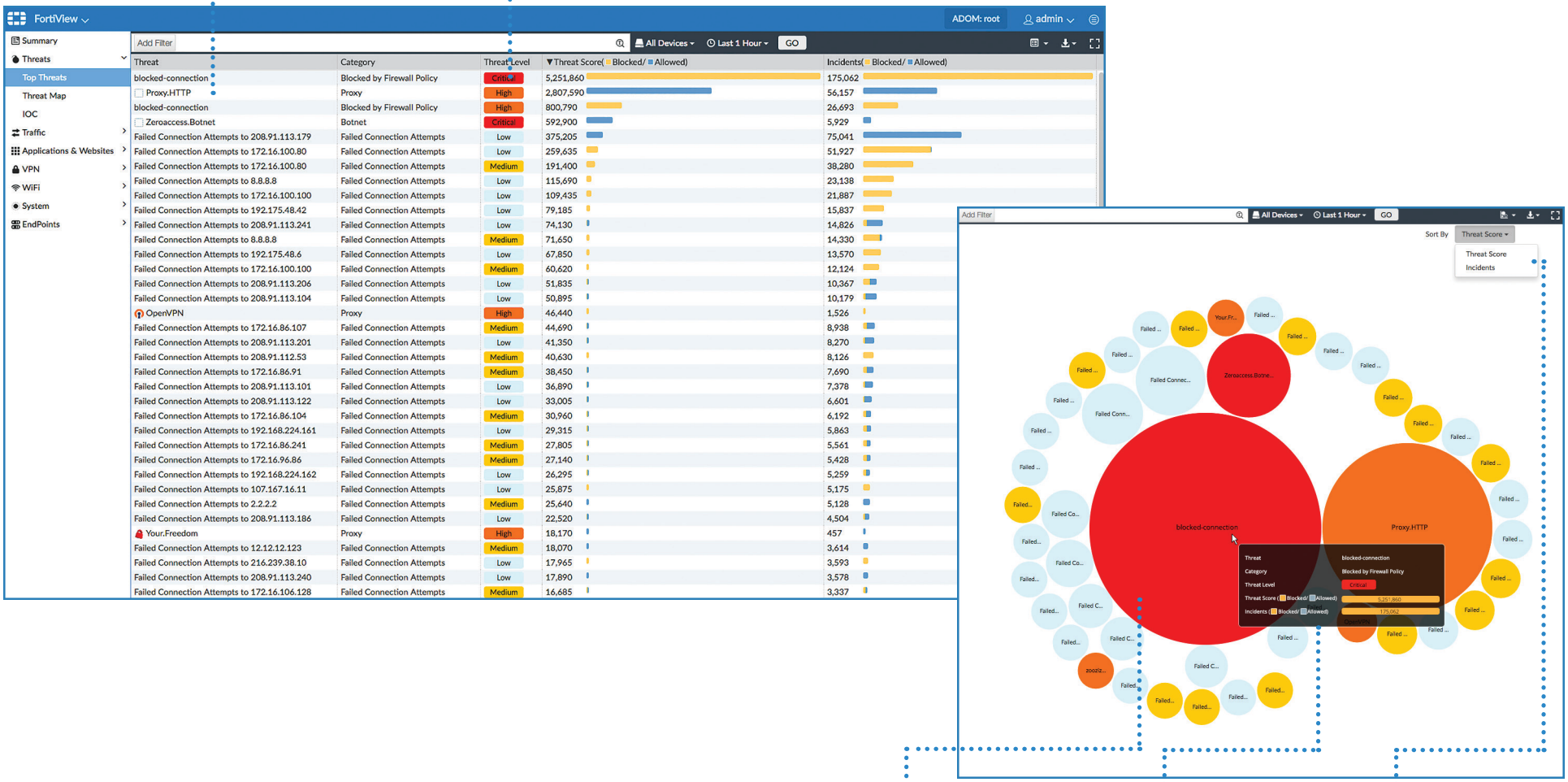
EICAR is the top threat to your network.

Torrent used the most bandwidth.

## Top Threats

Drill Down
Double-click the entry.

Sort Entries
Click a column heading.




Drill Down
Double-click the graphical element.

Get an Overview
Hover over a graphical element.

Sort Entries
Select from the drop-down menu.

## Filter Data in FortiView

Regular Search

Select a filter from the list and specify a value.

Advanced Search

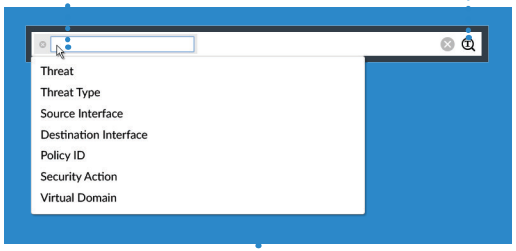
Click the icon to switch between regular and advanced search.

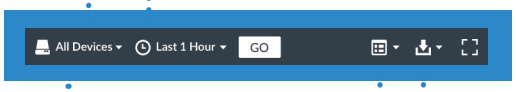
Filter by Device

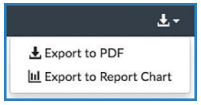
Select devices from the drop-down menu.

Filter by Time Period

Select a predefined time period or create a custom one.

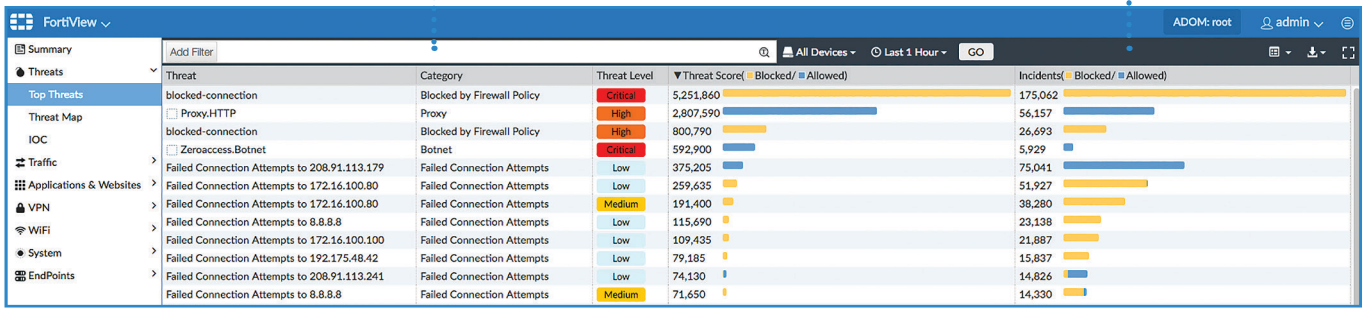


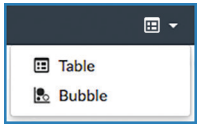




Export to Chart

Export a filtered Fortiview (or a drill-down) to charts, and save to the Chart Library.




FortiView Summary Formats

Use this drop-down menu to switch between different formats.

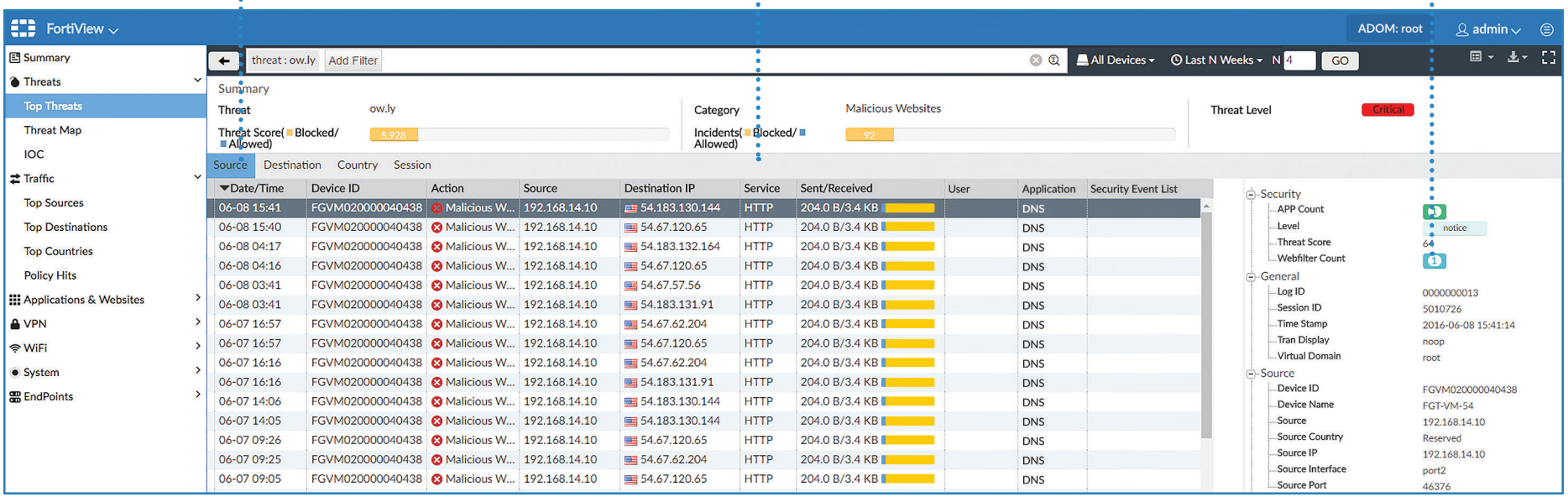
## Drill Down and View Log Details

Here is the drill-down view of threat ow.ly at log level.

View Data from Different Tabs
Click the corresponding tab.

View Log Details
Double-click a row to open the log detail pane in tree view.

View UTM Logs
Click the UTM log icon to open the UTM log view window.

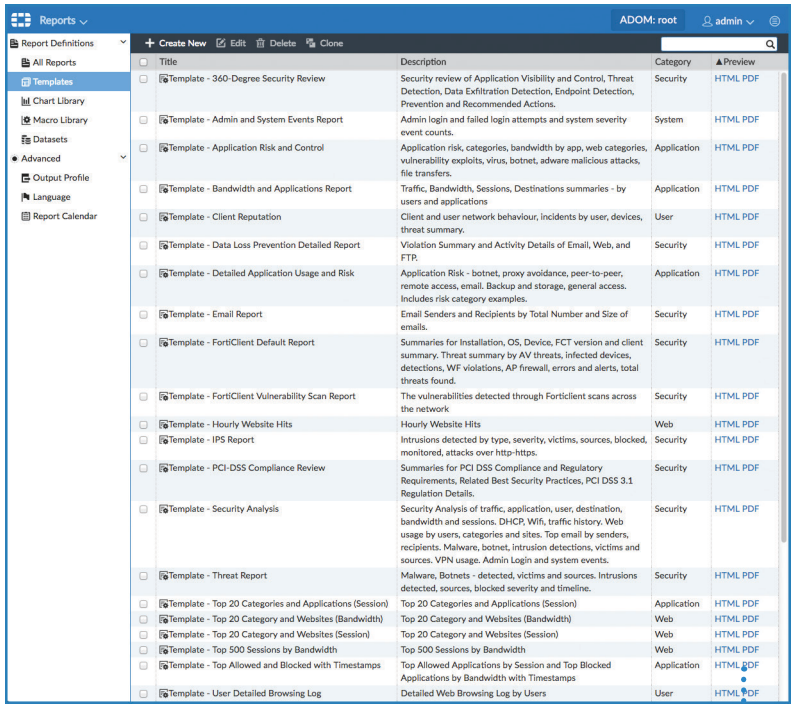


# 2 Generate Reports

FortiAnalyzer provides a comprehensive set of easily customizable report templates for you to quickly build reports.

## Predefined Report Templates

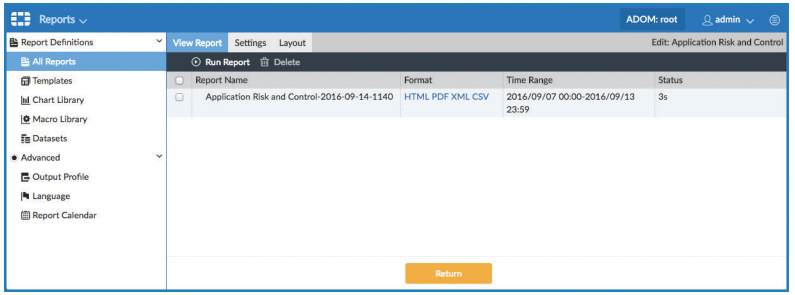
1. Go to **Reports > Report Definitions > Templates** to view the predefined report templates.




2. Click **HTML** or **PDF** in the preview column to view the sample report.

## Generate Reports

1. Go to **Reports > Report Definitions > All Reports**.
2. Double click the **Application Risk and Control** Report.
3. Click **Run Report** from the view report tab.
4. Once the report is generated, click on a format link to view and/or download it.

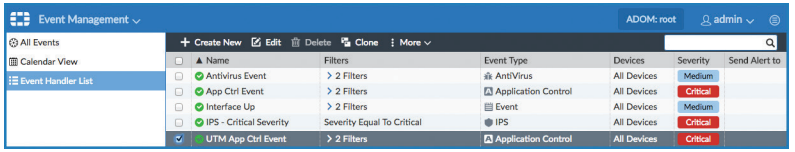



# 3 Monitor Events

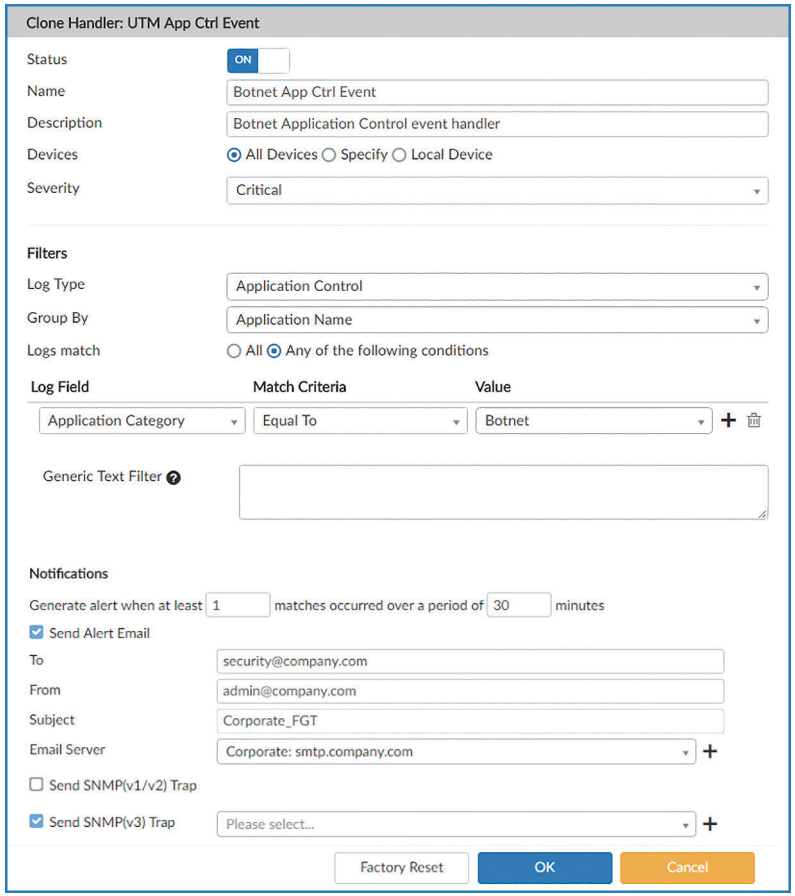
## Configure Event Handler

Events are triggered when the values of certain log fields meet the criteria defined in the Event Handlers. To create an event handler to catch the Botnet events:

1. Go to **Event Management > Event Handler Lists**.
2. Select the default handler: **UTM App Ctrl Event**.
3. Click **Clone**.



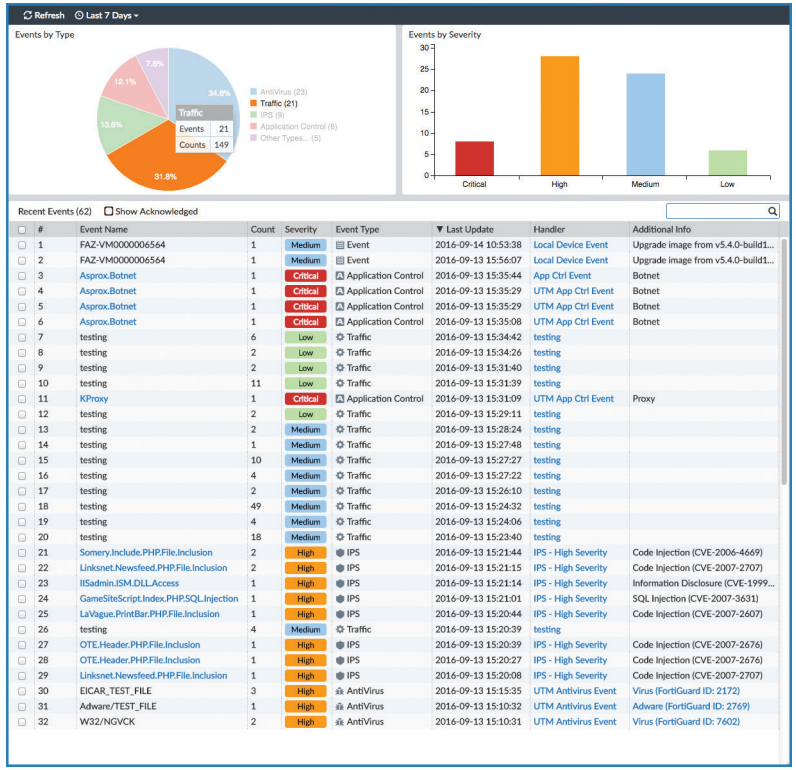
4. Enter a custom name.
5. Remove the application category **Proxy** from the matching criteria.
6. Click **OK** to save the handler.




## View Events

All triggered events are displayed on the event list page. To view events:

1. Go to **Event Management > All Events**.
2. Click an entry from the list to view more details.



# DAY 3: EXPLORE FURTHER

## Enable Event Notification

You can send alert notifications via Email, SNMP, to Syslog Server.

To configure notifications:

**Event Monitor > Event Handler List >** [Event Handler] **Edit**

## Create Custom Report

Create reports from predefined FortiAnalyzer templates, or use any of the 300+ predefined charts and 400+ datasets.

To create a custom report:

**Reports > All Reports > Create New**

## Monitor Storage Usage Graphs

Monitor FortiAnalyzer disk space, data policy, storage and disk utilization, as well as drill down to Analytic and Archive usage by device.

To monitor storage usage:

**Log View > Storage Statistics**

## System Dashboard Log Rate Widgets

Monitor logging rates and performance from the Dashboard. Useful widgets include **Insert Rate vs Receive Rate**, **Log Receive Monitor** and **Log Insert Lag Time**.

To add Widgets to monitor log rates:

**System Settings > Dashboard > Toggle Widgets**

## Indicators of Compromise for APT Detection

**FortiView > Threats > IOC**

For more information, see Administration Guide and videos in Fortinet Video Library

## LEARN MORE

FortiAnalyzer Administration Guide

http://docs.fortinet.com/fortianalyzer/admin-guides

Fortinet Document Library

http://docs.fortinet.com

Fortinet Video Guide

http://video.fortinet.com

Fortigate Cookbook

http://cookbook.fortinet.com

Training Services

http://www.fortinet.com/training

## SUPPORT AND FEEDBACK

Customer Service & Support

https://support.fortinet.com

Feedback on Fortinet technical document

Email: techdocs@fortinet.com

## FORTINET.COM